INE 5630
Segurança da Informação

- Plano de Ensino
- Introdução à Segurança da Informação
- Princípios de Criptografia
- Segurança de Redes
- Segurança de Sistemas

Parte I

- Segurança da Informação

Uma Visão Geral

Símbolos

- Símbolos: $S_1, S_2, \ldots, S_n$

  Um símbolo é um sinal (algo que tem um caráter indicador) que tem uma determinada forma, portanto, sendo algo baseado num conceito puramente sintático (forma).

  Exemplos: € H ¿ O T ? ? - ?

Símbolos

- A princípio, nada é dito sobre eles próprios.
- Tudo o que é assumido é que eles podem ser unicamente reconhecidos.

Dados

- Dado

  Um símbolo, mas considerando-se algum significado.

  Exemplos: ? ! % 5 = @ Ø

A informação de um símbolo

- Informação

  Um símbolo, mas considerando o significado (semântica), com relação a um contexto no qual o símbolo está inserido.

  Exemplos: ? ! % 5 = @ Ø

Alfabeto

- Um conjunto de símbolos: Alfabeto-Fonte.

  Exemplo 1: O conjunto de símbolos, representando as letras do alfabeto da língua inglesa ou da língua portuguesa.

Alfabeto

Exemplo 2:

O conjunto dos símbolos que representam os algarismos usados no sistema de numeração romano.

Alfabeto

Exemplo 3:

O conjunto dos símbolos que representam os algarismos usados nos sistemas de numeração binário, decimal ou hexadecimal.

Cadeias de Símbolos

- **Sequências de símbolos** de um alfabeto-fonte: $S_1, S_2, \ldots, S_n$

- $S_1S_2S_3S_4...S_n$ (cadeias, strings)
- palavras, números, códigos, ...
- Essas cadeias de símbolos, inseridas num determinado contexto, proporcionam alguma informação relevante a ser considerada.

Terminologia

- Existem certas palavras usadas nas terminologias da Teoria da Informação ou na terminologia dos Sistemas de Informação, tais como:

  “informação”, “transmissão”,
  “codificação”, “decodificação”

Terminologia

- Mas, um exame mais minucioso revelará que tudo o que é realmente assumido é uma **fonte de informação**, ou seja, uma sequência de símbolos $S_1, S_2, \ldots, S_n$ de um alfabeto-fonte.

Fontes de Informação

Na forma alfabética convencional:

- Um livro.
- Uma notícia formal impressa.
- Um relatório financeiro de uma empresa.

Fontes de Informação

Em forma não alfabética convencional:

- Uma dança.
- Uma música.
- Outras atividades humanas, com várias formas de símbolos para representar sua informação.
- Uma equação matemática.

Fontes de Informação

- Informação também existe em forma contínua. A natureza, geralmente, supre informação nessa forma.
- Mas, a prática moderna é amostrar o sinal contínuo em intervalos de tempo espaçados igualmente, e então digitalizar a quantidade observada (codificação).
- A informação pode, então, ser transmitida como um *stream* de dígitos binários.

Recursos da Informação

- Um arquivo.
- Objetos.
- Um banco de dados.

Valor da Informação

- Muitos **recursos de informação** que são disponíveis e mantidos em sistemas de informação distribuídos através de redes, têm um alto valor intrínseco para seus usuários.

- Toda informação tem valor e precisa ser protegida contra acidentes ou ataques.

Segurança da Informação

- Processo de proteção de informações:

  - **armazenadas em computadores** situados em **redes**;

  - **transportadas sobre essas**, através de canais de comunicação e dos mais diversos elementos de rede.

Problemas de Segurança da Informação

- Garantir que pessoas mal intencionadas não leiam ou, pior ainda, modifiquem mensagens enviadas a outros destinatários.

Problemas de Segurança da Informação

- Pessoas que tentam ter acesso a serviços remotos, os quais elas não estão autorizadas.

Problemas de Segurança da Informação

- Distinção entre uma mensagem supostamente verdadeira e uma mensagem falsa.
- Mensagens legítimas são capturadas e reproduzidas.
- Pessoas que negam ter enviado determinadas mensagens.

Soluções de Segurança da Informação

- Informações armazenadas em computadores situados em rede:
  - arquivos, objetos distribuídos,
  - aplicações na rede,
  - bancos de dados,
  - sistemas operacionais.
- Segurança do Computador

Soluções de Segurança da Informação

- Transportadas sobre redes:
  - através de canais de comunicação, dos mais diversos elementos de rede e protocolos.

- Criptografia (codificação e decodificação da informação transportada)
- Segurança de Rede

Segurança do Computador

- Segurança de Sistemas
  - Sistemas Operacionais
  - Bancos de Dados

- Segurança de Aplicações
  - Arquivos,
  - Objetos Distribuídos,
  - Agentes de Código Móvel

Objetivos da Segurança de Rede

- Diz respeito a tornar seguro os serviços providos numa rede, no sentido de:

  - não permitir que um cliente e um servidor interajam diretamente;
  - isolamento entre uma rede interna e a rede externa;

Objetivos da Segurança de Rede

- descobrir os pontos fracos, por onde se pode atacar numa rede;
- verificar quem está tentando entrar na rede, antes de revelar informações sigilosas ou entrar numa transação;

Objetivos da Segurança de Rede

- manter sigilo das informações que trafegam numa rede;
- certificar que uma mensagem recebida é legítima;
- provar o envio de uma mensagem;

Objetivos da Segurança de Rede

- detectar invasões numa rede;
- disfarçar os verdadeiros recursos da rede, visando o isolamento de um atacante;
- cuidar da privacidade da informação.

Segurança de Sistemas

- Invasão por usuário:

  Pode tomar a forma de acesso não autorizado a uma máquina, com aquisição de privilégios ou execução de ações além daquelas autorizadas.

Segurança de Sistemas

- Invasão por software:

  Pode tomar a forma de um Vírus, um Worm (verme) ou um Cavalo de Tróia.

Segurança de Sistemas

- Invasão por Usuário
- Invasão por Software

- Todos esses ataques são relacionados à segurança de rede, porque a entrada num sistema pode ser alcançada por meio de uma rede.

Segurança de Sistemas

- Contudo, esses ataques não estão confinados a ataques baseados na rede (que precisam da rede).

- Um usuário com acesso a um terminal local pode tentar invadir sem usar uma rede.

Segurança de Sistemas

- Por exemplo, um Vírus ou um Cavalo de Tróia pode ser introduzido dentro de um sistema por meio de um disquete.

- Somente um Worm é que necessita da rede.

Segurança de Sistemas

- Assim, invasão de sistema é uma área na qual os interesses para segurança de rede e segurança do computador se sobrepõem.

Segurança da Informação

- Proteção de informações para que sejam mantidos os aspectos de confidencialidade, integridade e disponibilidade.

Segurança da Informação

- É uma disciplina complexa e pode abranger várias situações, tais como:
  - Erros,
  - Acesso indevido,
  - Furto,
  - Fraude,
  - Sabotagem e Causas da Natureza.

Segurança da Informação

- Define-se como o processo de proteção de informações armazenadas em computadores situados em redes.

Segurança da Informação

- Com o advento das redes de computadores e a intensificação do uso dessas pelas empresas, a segurança da informação tem sido um assunto que vem exigindo, cada vez mais, maiores cuidados do que aqueles até então existentes antes das redes.

Mercado

- Segurança voltada para o mercado corporativo: tecnologias avançadas com alta capacidade de tráfego e gerenciamento dos recursos de informação.

- Segurança voltada para o mercado doméstico: usuário da Internet.

Mercado Corporativo

- A Segurança da Informação pode ser estudada visando-se:
- Segurança de Redes: Criptografia, Autenticação, Protocolos, Plataformas.
- Segurança de Sistemas e das Aplicações: OS, BD e protocolos específicos.

Segurança da Informação

- Porque ...

  os sistemas computacionais ou de comunicação, que armazenam ou transmitem informação são vulneráveis (sujeito a intrusões).

O Conceito de Intrusão

- Análise da **Vulnerabilidade** (descobrir o melhor caminho para chegar até a invasão).
- Preparação das **Ferramentas** (constrói ou escolhe as ferramentas para a invasão).
- **Ameaça** ou Tentativa (quando o invasor pula o muro).
- **Ataque** (concretiza o arrombamento).
- **Invasão** ou Penetração (quando obtém sucesso).

Vulnerabilidade

- “Pontos Fracos”
- Probabilidade de uma ameaça transformar-se em realidade.
- Uma falha de segurança em um sistema de software ou de hardware que pode ser explorada para permitir a efetivação de uma intrusão.

Ameaça (Threat)

- “Pulando o Muro”
- Uma ação ou evento que pode prejudicar a segurança.
- É a tentativa de ataque a um sistema de informação, explorando suas vulnerabilidades, no sentido de causar dano à confidencialidade, integridade ou disponibilidade.

Ataque (Attack)

- “Arrombamento”
- O ato de tentar desviar dos controles de segurança de um sistema de informação.
- Qualquer ação que comprometa a segurança da informação de propriedade de uma organização.

Ataques

- Pode ser ativo, tendo por resultado a alteração dos dados.
- Pode ser passivo, tendo por resultado a obtenção da informação (escuta oculta de transmissões): liberação de conteúdos de mensagens, análise de tráfico)

Ataques

- Pode ser externo, quando originado de fora da rede protegida.
- Pode ser interno, quando originado de dentro da rede protegida.

Ataques

- O fato de um ataque estar acontecendo, não significa necessariamente que ele terá sucesso.

- O nível de sucesso depende da vulnerabilidade do sistema ou da atividade e da eficiência das contramedidas de segurança existentes (se não forem suficientemente eficientes).

Intrusão ou Invasão

- Sucesso no ataque.
- Obtenção da Informação.
- Acesso bem sucedido, porém não autorizado, em um sistema de informação.

Contramedidas

- Mecanismos ou procedimentos colocados num sistema para reduzir riscos.

- Riscos são provenientes de vulnerabilidades, ameaças, e ocasionam impacto.

Ativos da Informação

- ***Asset*** *(Ativo)* - Tudo que faz parte da operação de um sistema ou desenvolvimento
- Exemplo: hardware, software, documentação, equipe e dados.

Riscos de Segurança

- Risco é a probabilidade da ocorrência de uma ameaça particular.

Análise de Risco

- Análise de Riscos – Identificação e avaliação dos riscos que os recursos da informação estão sujeitos.

Gerenciamento de Riscos

- O processo total de identificar, de controlar e minimizar os riscos que podem afetar os recursos de informação do sistema.

Gerenciamento de Riscos

- Inclui a análise de risco, a análise de custo-benefício, a avaliação de segurança das proteções e a revisão total da segurança.

Risco Residual

- Riscos ainda existentes depois de terem sido aplicadas medidas de segurança.

Impacto

- A consequência para uma organização da perda de confidencialidade, disponibilidade e (ou) integridade de uma informação.

Impacto

- O impacto deve ser analisado quanto à modificação, destruição, divulgação ou negação de informação.

- Relaciona-se a imagem da empresa, ao dano, a perdas financeiras ou legais e a outros problemas que podem ocorrer como consequência de uma ruptura da segurança.

Os Requisitos de Segurança

- Disponibilidade
- Privacidade (**)
- Confidencialidade
- Integridade
- Autenticidade
- Controle de Acesso
- Não-Repúdio da Informação

Segurança da Informação

- Assim, a disciplina de segurança da Informação trata de garantir a existência dos requisitos fundamentais para proporcionar um nível aceitável de segurança nos recursos de informação.

Segurança da Informação

- De uma forma mais simplificada:

- Proteção de informações para que sejam mantidos os requisitos de:
  - confidencialidade,
  - integridade,
  - disponibilidade.

Segurança da Informação

- Definir restrições aos recursos da informação.
- Segurança da Informação é a gestão de tais restrições.
- Para gerir restrições é preciso definir políticas de segurança.
- Um conjunto de políticas de segurança define um Modelo de Segurança.

Disponibilidade (Availability)

- É o requisito de segurança em que a informação deve ser entregue para a pessoa certa, no momento que ela precisar.
- A informação estará disponível para acesso no momento desejado.
- Proteção contra interferência como meio para acessar os recursos.

Privacidade (Privacy)

- É o requisito de segurança em que a informação pode ser fornecida, mas somente com a autorização do proprietário da informação.

- Informações médicas ou financeiras.

Confidencialidade

- É o requisito de segurança que visa a proteção contra a revelação de informação a indivíduos não autorizados.

- Garante que a informação em um sistema, ou a informação transmitida são acessíveis somente a partes autorizadas.

Integridade

- É o requisito de segurança que visa a proteção da informação contra modificações não autorizadas.

- Garante que somente partes autorizadas podem modificar a informação. Modificação inclui: escrever, mudar, mudar status, apagar, criar e atrasar ou responder mensagens.

Autenticidade

- É o requisito de segurança que visa validar a identidade de um usuário, dispositivo, ou outra entidade em um sistema, frequentemente como um pré-requisito a permitir o acesso aos recursos de informação no sistema.

Autenticidade

- Garante que a origem da informação é corretamente identificada, assegurando que a identidade não é falsa.

Acesso

- Interação entre um usuário e o sistema que permite a informação fluir de um para o outro.

Controle de Acesso

- Procedimentos operacionais de gerenciamento para detectar e prevenir acessos não autorizados e permitir acessos autorizados num sistema.

Não-Repúdio

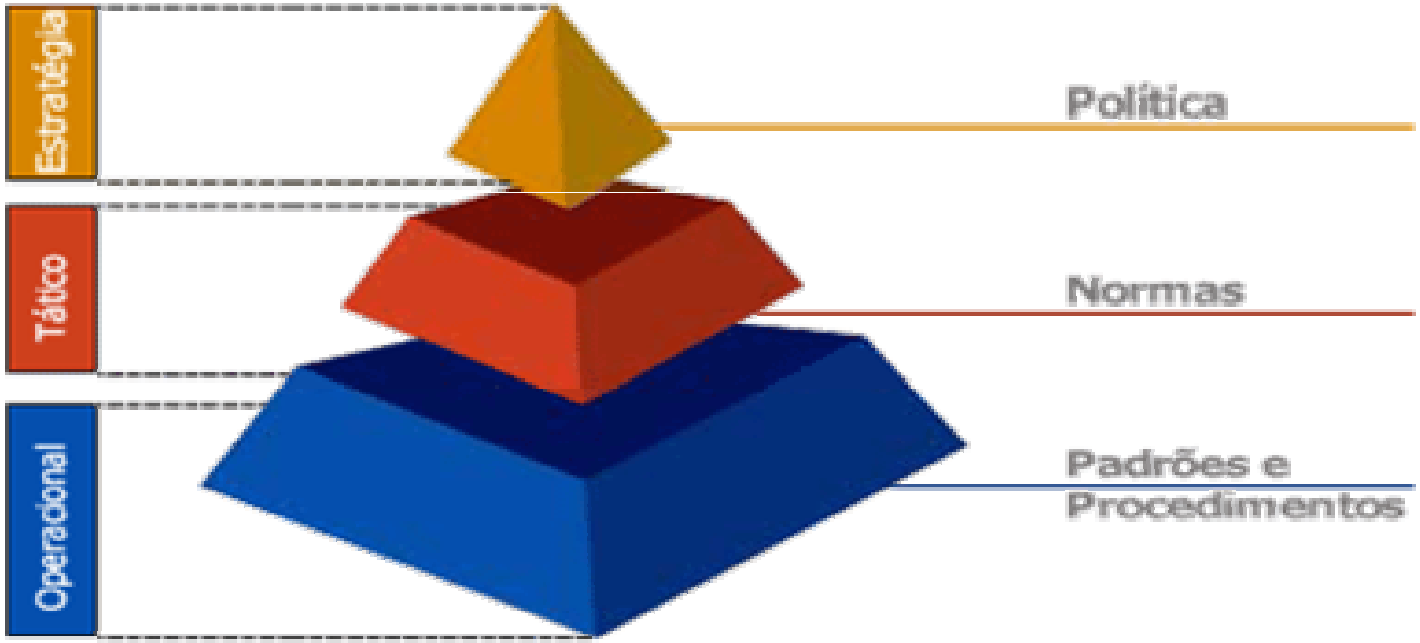
- Requer que nem o transmissor nem o receptor da informação, possam negar o envio da informação.

- O sistema não permite a negação, por parte do usuário, do envio de determinada informação.

O que é Segurança da Informação
(Exemplo BRADESCO)

- A segurança da informação é um conjunto de medidas que se constituem basicamente de controles e política de segurança, tendo como objetivo a proteção das informações dos clientes e da empresa, controlando o risco de revelação ou alteração por pessoas não autorizadas.

Segurança da Informação (Fonte BRADESCO)



Nível de Estratégia

Estratégia

É o nível que refere-se às Politicas da Organização e descreve "o que deve ser feito".

Nível Tático

Tático

É o nível que refere-se às Normas da Organização e com base nas Políticas, descreve as "regras" a serem adotadas.

Nível Operacional

Operacional

É o nível dos Procedimentos da Organização e com base nas Normas, descreve "como serão implementadas as regras".

Política de Segurança (Exemplo BRADESCO)

- Política de Segurança é um conjunto de diretrizes que definem formalmente as regras e os direitos dos funcionários e prestadores de serviços, visando à proteção adequada dos ativos da informação.

Base da Política
(Exemplo BRADESCO)

- Essa política está baseada em diretrizes de segurança e diretivas de privacidade.

Diretrizes de Segurança (Exemplo do BRADESCO)

- Proteger as informações
- Assegurar Recursos
- Garantir Proteção
- Garantir Continuidade
- Cumprir Normas
- Atender às Leis
- Selecionar Mecanismos
- Comunicar Descumprimento

Diretivas de Privacidade (Exemplo BRADESCO)

- O Banco Bradesco esclarece como as informações dos clientes são armazenadas em seus computadores, garantindo: confidencialidade, integridade e disponibilidade.

Confidencialidade: Propriedade de manter a informação a salvo de acesso e divulgação não autorizados.

Disponibilidade: Propriedade de manter a informação disponível para usuários, quando estes dela necessitarem.

Integridade: Propriedade de manter a informação acurada, completa e atualizada.

Diretivas de Privacidade (Exemplo do BRADESCO)

- **As informações de nossos clientes seguem as seguintes diretivas:**
- As informações são coletadas de forma legal e sob o conhecimento do usuário;
- As informações são enviadas ao Bradesco de forma segura com métodos de criptografia e certificação digital;
- As informações enviadas ao Bradesco serão armazenadas de forma íntegra, sem alteração de qualquer parte;
- As informações são armazenadas de forma segura e criptografada restringindo o acesso somente às pessoas autorizadas;
- As informações serão utilizadas apenas para as finalidades aprovadas pela Organização;
- As informações dos clientes nunca serão fornecidas a terceiros, exceto por determinação legal ou judicial.

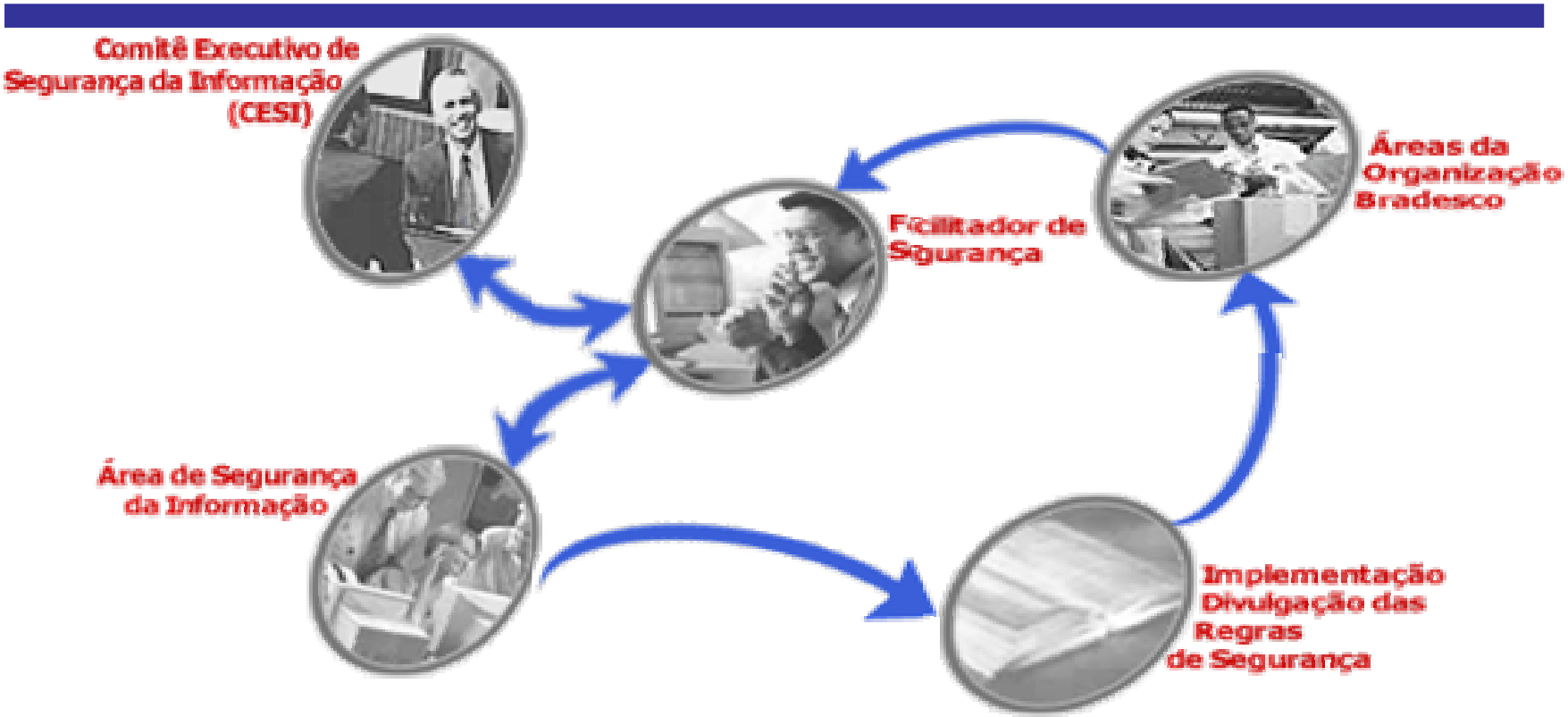
Processo de Segurança e Acompanhamento (BRADESCO)

- O processo de segurança da informação pode ser melhor ilustrado, conforme o ciclo abaixo:


Análise de Segurança
Definição Atualização de Regras de Segurança
Implementação Divulgação das Regras de Segurança
Administração de Segurança
Auditorias
RELATÓRIO
Ciclo de Segurança

Organização da Segurança (EXEMPLO BRADESCO)

- A Organização Bradesco definiu uma estrutura formal, com objetivos e responsabilidades específicas, para tratar da segurança da informação de uma forma adequada.
- O objetivo dessa estrutura é definir, manter e melhorar a segurança da informação no ambiente da Organização Bradesco.


Comitê Executivo de Segurança da Informação (CESI)
Facilitador de Segurança
Áreas da Organização Bradesco
Área de Segurança da Informação
Implementação Divulgação das Regras de Segurança

Infra Estrutura de Segurança da Informação (1)

O **projeto de segurança** da informação pode ser definido como segue:

- **Análise de riscos.**
- Criação de uma **política de segurança corporativa.**
- Processo de **conscientização do pessoal** de informática e demais usuários.
- Proteção contra **softwares maliciosos.**

Infra Estrutura de Segurança da Informação (2)

- **Firewall e Hosts de Segurança;**
- Sistemas de **Criptografia (Protocolos de Segurança).**
- Sistemas de **Detecção de Intrusão.**
- Sistemas de **Análise de Vulnerabilidades.**
- Ferramentas de **Autenticação** de Usuários: **assinaturas digitais**, **certificação digital.**
- Procedimentos de **Auditoria.**
- **Aspectos Jurídicos .**